UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

CHRISTINA LESLIE,
Individually and on behalf of all others similarly situated,

Plaintiff,

v.

THOMPSON REUTERS CORPORATION,

Defendant.

Case No: 1:22-CV-07936

Judge Jennifer H. Reardon~~:~~

JURY TRIAL REQUESTED

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Christina Leslie, individually and on behalf of all others similarly situated, ~~files this Class Action Complaint against~~ respectfully submits this First Amended Class Action Complaint against Defendant Thompson Reuters Corporation ("Defendant") for violations of the federal Video Privacy Protection Act, 18 U.S.C. § 2710 ("VPPA").

Plaintiff's claims arise from Defendant's practice of using tracking software programs developed by Facebook to knowingly ~~disclosing~~ disclose her personally identifiable information to a third party, Meta Platforms, Inc. (owner of Facebook and Instagram, as well as other applications), in a form of Meta's choosing given it programmed the software. This personally identifiable information ~~("Facebook"),~~ data ~~containing~~ contains Plaintiff's and other digital-subscribers Class Members' (i) personally identifiable information or Facebook ID ("FID") and (ii) the computer file containing video and its corresponding URL viewed ("Video Media") (collectively, "Personal Viewing Information").

In other words, this transmission of Personal Viewing Information to Facebook is achieved through Defendant's adoption of the "Facebook pixel" which Facebook designed in such a way to allow third parties to determine what data it will collect from its users and transmit

back to Facebook from a menu of options, Defendant chooses how it will use the pixel, including what video viewing information is transmitted, when (or what event triggers) data transmission, and the form in which said data is transmitted back to Facebook. The information related to the pre-recorded videos that are watched and then transmitted back to Facebook to link it to the individual using the Facebook ID so it can then be capitalized on by Defendant to push out more content and advertisements it feels the user be interested in based on the ever-evolving Facebook profile.

~~Plaintiff's allegations are made on personal knowledge as to Plaintiff and Plaintiff's own acts and upon information and belief as to all other matters.~~

NATURE OF THE ACTION

1. This is a consumer digital privacy class action complaint against Thompson Reuters Corporation, as the owner of ~~R~~www.reuters.com, for violating the VPPA by disclosing its digital subscribers' identities and Video Media to Facebook without the proper consent.

~~1.~~2. Digital subscribers of reuters.com are "consumers" under the VPPA.

~~2.~~3. The VPPA prohibits "video tape service providers," such as www.r~~R~~euters.com, from knowingly disclosing consumers' personally identifiable information, including "information which identifies a person as having requested or obtained specific video materials or services from a video tape provider," without express consent in a stand-alone consent form.

~~3.~~4. Like other businesses with an online presence, Defendant collects and shares the personal information of visitors to its website and mobile application ("App") with third parties. Defendant does this through cookies, software development kits ("SDK"), and pixels. In other words, digital subscribers to www.~~R~~reuters.com have their personal information disclosed to Defendant's third-party business partners.

~~4.~~5. The Facebook pixel is a code developed by Facebook that Defendant installed on ~~R~~reuters.com allowing it to collect users' data, share that data with Facebook in real time in a form that Facebook controls, and, in return, receive information about its users' identity linked to the Facebook ID and that individual user's video-watching habits.~~.~~ More specifically, it tracks when digital subscribers enter www.r~~R~~euters.com or www.r~~R~~euters.com's accompanying App and view Video Media. ~~R~~www.reuters.com tracks and discloses to Facebook the digital subscribers' viewed Video Media, and most notably, the digital subscribers' FID which provides any reasonable person access to a person's Facebook (and Instagram) page and/or account which in turn provides that person with access to information such as the person's name, location of residence, work history, educational history, date of birth, photographs of the user that include metadata sufficient to demonstrate location, gender, and likes~~.~~ This occurs even when the digital subscriber has not shared (nor consented to share) such information.

~~5.~~6. Importantly, Defendant shares the Personal Viewing Information – *i.e.*, digital subscribers' unique FID and video content viewed – together as one data point to Facebook. Because the digital subscriber's FID uniquely identifies an individual's Facebook user account, Facebook—or any other ordinary person—can use it to quickly and easily locate, access, and view digital subscribers' corresponding Facebook profile. Put simply, the pixel allows Facebook to know what Video Media one of its users viewed on www.r~~R~~euters.com.

~~6.~~7. Thus, without telling its digital subscribers, Defendant profits handsomely from its unauthorized disclosure of its digital subscribers' Personal Viewing Information to Facebook. It does so at the expense of its digital subscribers' privacy and their statutory rights under the VPPA.

~~7.~~8. Because www.r~~R~~euters.com digital subscribers are not informed about this dissemination of their Personal Viewing Information – indeed, it is automatic and invisible – they cannot exercise reasonable judgment to defend themselves against the highly personal ways r~~R~~euters.com has used and continues to use data it has about them to make money for itself.

~~8.~~9. Defendant chose to disregard Plaintiff's and hundreds of thousands of other ~~R~~reuters.com digital subscribers' statutorily protected privacy rights by releasing their sensitive data to Facebook. Accordingly, Plaintiff brings this class action for legal and equitable remedies to redress and put a stop to Defendant's practices of intentionally disclosing its digital subscribers' Personal Viewing Information to Facebook in knowing violation of VPPA.

JURISDICTION AND VENUE

~~9.~~10. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over the claims that arise under the Video Privacy Protection Act, 18 U.S.C. § 2710.

~~10.~~11. This Court also has jurisdiction under 28 U.S.C. § 1332(d) because this action is a class action in which the aggregate amount in controversy for the proposed Class (defined below) exceeds $5,000,000, and at least one member of the Class is a citizen of a state different from that of Defendant.

~~11.~~12. Venue is appropriate in this District pursuant to 28 U.S.C. § 1391 because Defendant does business in and is subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claim occurred in or emanated from this District.

THE PARTIES

~~12.~~13. Plaintiff Christina Leslie is an adult citizen of the State of California and is domiciled in the State of California. Plaintiff began a digital subscription to www.~~R~~reuters.com in 2022 which continues to this day. Plaintiff has had a Facebook account from approximately

2012 to the present. During the relevant time period she has used her ~~R~~ www.reuters.com digital subscription to view Video Media through www.r~~R~~euters.com and/or App while logged into her Facebook account. By doing so, Plaintiff's Personal Viewing Information was disclosed to Facebook pursuant to the systematic process described herein. Plaintiff never gave Defendant express written consent to disclose her Personal Viewing Information.

14. ~~13.~~ Defendant Thompson Reuters Corporation:

a. Is a publicly traded multinational media conglomerate headquartered in Toronto, Canada.

b. Is one of the leading news sources in the world and claims to be read and seen by 1 billion people each day.~~0F~~[1]

c. Reuters.com has approximately 33 million unique monthly visitors.[2]~~1~~

d. Had an annual revenue of $1.7 billion in 2021.~~1F~~[3]

e. Reuters.com includes a Videos section which provides a broad selection of video content.

f. Combined, Thompson Reuters Corporation and ~~R~~reuters.com are used by numerous U.S. digital media viewers.

g. Through ~~R~~reuters.com and App, Defendant delivers and, indeed, is in the business of delivering countless hours of video content to its digital subscribers.

FACTUAL ALLEGATIONS

A. Background of the Video Privacy Protection Act

[1] *See* Reuters The Facts, *available at* https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/reuters-news-agency/fact-sheet/reuters-fact-sheet.pdf (last visited ~~Sept. 02, 2022).~~May 27, 2025)

[2] *Id.*

[3] *See* Thomson Reuters Reports Fourth-Quarter and Full-Year 2021 Results (Feb. 8, 2022), *available at* https://www.thomsonreuters.com/en/press-releases/2022/february/thomson-reuters-reports-fourth-quarter-and-full-year-2021-results.html (last visited May 27, 2025)~~(last visited Sept. 02, 2022).~~

~~14.~~15. The VPPA generally prohibits the knowing disclosure of a customer's video rental or sale records without the informed, written consent of the customer in a form "distinct and separate from any form setting forth other legal or financial obligations." Under the statute, the Court may award actual damages (but not less than liquidated damages of $2,500.00 per person), punitive damages, equitable relief, and attorney's fees.

~~15.~~16. The VPPA was initially passed in 1988 for the explicit purpose of protecting the privacy of individuals' and their families' video rental, purchase and viewing data. Leading up to its enactment, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." S. Rep. No. 100-599 at 7-8 (1988).

~~16.~~17. Senators at the time were particularly troubled by disclosures of records that reveal consumers' purchases and rentals of videos and other audiovisual materials. As Senator Patrick Leahy and the late Senator Paul Simon recognized, records of this nature offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

~~17.~~18. In proposing the Video and Library Privacy Protection Act (later codified as the VPPA), Senator Leahy stated that "[i]n practical terms our right to privacy protects the choice of movies that we watch with our family in our own homes. And it protects the selection of books that we choose to read." 134 Cong. Rec. S5399 (May 10, 1988). Thus, the personal nature of such information, and the need to protect it from disclosure, is the inspiration of the statute: "[t]hese activities are at the core of any definition of personhood. They reveal our likes and

dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id*.

~~18.~~19. While these statements rang true in 1988 when the VPPA was passed, the importance of legislation like the VPPA in the modern era of data mining from online activities is more pronounced than ever before. During a recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy emphasized the point by stating: "While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."~~2F~~[4]

20. In 2012, with emergence of the internet in mind, Congress amended and updated the VPPA, and in doing so, reiterated the Act's applicability to "so-called 'on-demand' cable services and Internet streaming services [that] allow consumers to watch movies or TV shows on televisions, laptop computers, and cell phones." S. Rep. 112-258, at 2.

21. The 2012 amendments clarified that statute "that a video tape service provider may obtain a consumer's informed, written consent on an ongoing basis and that consent may be obtained through the Internet." Video Privacy Protection Act Amendments Act of 2012, Pub. L. 112-258, 126 Stat. 2414; *see also* 18 U.S.C. § 2710(b)(2)(B) (authorizing a video tape service provider to disclose consumers' personally identifiable information "to any person with the informed, written consent (including through an electronic means using the Internet) of the

[4] *See* Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, https://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21st-century (last visited Sept. 02, 2022).

consumer" provided either "at the time the disclosure is sought" or "in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner").

22. The consent, however, must be "in a *form distinct and separate* from any form setting forth other legal or financial obligations of the consumer." 18 U.S.C. § 2710(a)(4) (emphasis added).

23. The VPPA prohibits "[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider." 18 U.S.C. § 2710(b)(1).

24. The VPPA defines "consumer" as any "renter, purchase, or subscriber of goods of services from a video tape service provider." 18 U.S.C. § 2710(a)(1).

25. Under the VPPA, a consumer does not have to spend money for a good or service to be a "subscriber." *Salazar v. Nat'l Basketball Ass'n*, 118 F.4th 533, 551 (2d Cir. 2024).

26. The VPPA defines personally identifiable information ("PII") as "information which identifies a person as having requested or obtained specific video materials or services from a video service provider." 18 U.S.C. § 2710(a)(3).

27. By transmitting Facebook-specific identifiers (i.e., Facebook IDs) and video file names through Facebook's own embedded tool, the disclosing party, here, Defendant, expressly instructed Facebook as to the exact videos and other content the consumer accessed.

~~19.~~ The Facebook Pixel is one of the most, if not the most, commonly used, known, and easily understood tracking pixels that link individual users to their internet activities.

28.

29. The Facebook Pixel is designed to allow any ordinary person (as long as we can presume an "ordinary person" can read), to read and understand the contents of information being shared with Facebook as the title of the video is clearly decipherable since it appears in plain English.

30. Even though some of the information disclosed is technical in nature, any ordinary person can easily surmise what video content a person requested or obtained because it directly tracks the name of the video as it appears on the user's screen, as well as that person's FID, as it is an easily identifiable and unique string of numbers tied to an individual.

31. In other words, the disclosure was purposefully structured to be technical in nature – given the vast amount of data that entities including Defendant seek to disclose to Facebook.

32. However, even though the disclosure is technical, it can be easily understood by ordinary people, as the general population understands how hyperlinks and URLs work.

33. Further, it is generally understood that when marketing a product or service, knowing your target audience is a fundamental aspect.

~~20.~~ As such, it is generally understood that the Pixel would receive, decipher, and link data, including data protected by the VPPA, to an individual's Facebook Profile.

34.

35. Indeed, Facebook not only received this information in the precise form it was transmitted but also leveraged it to build detailed profiles for targeted advertising based on a consumer's video-watching habits. Specifically, The Facebook Pixel transmits data via HTTP requests (e.g., through GET requests) that include URL-encoded query parameters. Facebook's own documentation assumes that URL data will be encoded with UTF-8 before being appended

to the GET request. *See*, https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/ (last visited June 5, 2025). Stated differently, Facebook receives URL data in a form that is easily converted to data strings that humans can read. ~~Indeed, Facebook not only received this information in the precise form it was transmitted but also leveraged it to build detailed profiles for targeted advertising based on a consumer's video-watching habits.~~

36. A video tape service provider is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

37. Under the VPPA, "[a]ny person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court." 18 U.S.C. § 2710(c)(1).

38. Under the VPPA, "[t]he court may award—(A) actual damages but not less than liquidated damages in an amount of $2,500; (B) punitive damages; (C) reasonable attorneys' fees and other litigation costs reasonably incurred; and (D) such other preliminary and equitable relief as the court determines to be appropriate." 18 U.S.C. § 2710(c)(2).

39. The VPPA itself requires video tape service providers like Defendant to "destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected." 18 U.S.C. § 2710(e).

40. This would mean, for instance, that when a user deletes their account, Defendant no longer has a use for the information and should delete it as soon as practicable. But Defendant's policies indicate it does not delete said information after no longer having a use for it, let alone the third parties to whom it discloses PII.

~~21.~~41. In this case, Defendant chose to deprive Plaintiff and the Class members of that right by knowingly and systematically disclosing their Personal Viewing Information to Facebook, without providing notice to (let alone obtaining consent from) anyone, as explained herein.

B. Reuters.com's Digital Subscriptions

~~22.~~42. To register for ~~R~~ www.reuters.com, users sign up for an online newsletter. www.~~R~~reuters.com users provide their personal information, including but not limited to their name, email address, and zip code.

~~23.~~43. Thompson Reuters Corporation operates a website in the U.S. accessible from a desktop and mobile device at www.r~~R~~euters.com. It also offers an App available for download on Android and iPhone devices.

~~24.~~44. On information and belief, all digital subscribers provide Defendant with their IP address, which is a unique number assigned to all information technology connected devices, that informs Defendant as to subscribers' city, zip code and physical location.

~~25.~~45. Digital subscribers may provide to Defendant the identifier on their mobile devices and/or cookies stored on their devices.

~~26.~~46. When opening an account, Defendant does not disclose to its digital subscribers that it will share their Personal Viewing Information with third parties, such as Facebook. Digital subscribers are also not asked to consent to such information sharing upon opening an account.

~~27.~~47. After becoming a digital subscriber, viewers have access to a variety of ~~R~~ www.reuters.com Video Media on Defendant's digital platform.

48. Notably, once a digital subscriber signs in and watches ~~R~~ www.reuters.com Video Media, the digital subscriber is not provided with any notification that their Personal

Viewing Information is being shared. Similarly, Defendant also fails to obtain digital subscribers' written consent to collect their Personal Viewing Information "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer," as the VPPA requires.

~~Similarly, Defendant also fails to obtain digital subscribers' written consent to collect their Personal Viewing Information "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer," as the VPPA requires.~~

~~28.~~49.

C. Defendant Admits It Collects and Discloses Certain Personal Information of Digital Subscribers to Third Parties But Fails to Advise It Discloses Personal Viewing Information, as Required Under the VPPA.

~~29.~~50. The operative Privacy Policy for ~~R~~ www.reuters.com states that it collects "Personal Information" from its users:

> "Generally, we collect the following categories of personal information: …Usage Information and Browsing History, such as usage metrics (including usage rates, occurrences of technical errors, diagnostic reports, settings preferences, backup information, API calls, and other logs), content interactions (including searches, views, downloads, prints, shares, streams, and display or playback details), and user journey history (including clickstreams and page navigation, URLs, timestamps, content viewed or searched for, page response times, page interaction information (such as scrolling, clicks, and mouse-overs), and download errors), advertising interactions (including when and how you interact with marketing and advertising materials, click rates, purchases or next steps you may make after seeing an advertisement, and marketing preferences), and similar data."~~3F~~[5]

[5] *See* Thomson Reuters Privacy Statement, *available at* https://www.thomsonreuters.com/en/privacy-statement.html (last visited Sept. ##, 2022).

~~30.~~51. Reuters.com discloses in its Privacy Policy that it automatically collects "content interactions (including searches, views, downloads, prints, shares, streams, and display or playback details)."~~4F~~[6]

~~31.~~52. Importantly, nowhere in www.r~~R~~euters.com's Terms of Service or Privacy Policy is it disclosed that Defendant will share digital subscribers' private and protected Personal Viewing Information with third parties, including Facebook.

D. How Reuters.com Disseminates Digital Subscribers' Personal Viewing Information

1. Tracking Pixels

53. Approximately seven-in-ten U.S. citizens have a Facebook profile[7] – – all of whom provided the same personal information to Meta when creating their Facebook profiles.

54. Meta promotes its ability to allow businesses to target their ads to specific audiences using these types of identifying information[8] as well as information about actions specific users have taken on the businesses' websites.[9]

~~32.~~55. Websites and apps use Facebook's pixel and SDK to collect information about user's devices and activities and send that to Facebook. Facebook then uses that information to show the user targeted ads.

---

[6] *See id.*

[7] Schaeffer, Katherine, Pew Research Center, *5 Facts about how Americans use Facebook, two decades after its launch* (Feb. 2, 2024), *available at* https://www.pewresearch.org/short-reads/2024/02/02/5-facts-about-howamericans-use-facebook-two-decades-after-its-launch/ (last visited June 3, 2025).

[8] Meta Business Help Center, Age and gender, Meta, *available at* https://www.facebook.com/business/help/151999381652364 (last visited June 3, 2025); *see also* Meta Business Help Center, About specific targeting, Meta, *available at* https://www.facebook.com/business/help/121933141221852?id=176276233019487 (last visited June 3, 2025).

[9] Meta Business Help Center, Options to create a website custom audience, Meta, *available at* https://www.facebook.com/business/help/2539962959620307 (last visited Oct. 15, 2024).

56. The Facebook tracking pixel, also known as a "tag" or "web beacon" among other names, is an invisible tool that tracks consumers' actions on Facebook advertisers' websites and reports them to Facebook. It is a version of the social plugin that gets "rendered" with code from Facebook. To obtain the code for the pixel, the website advertiser tells Facebook which website events it wants to track (*e.g.*, Video Media) and Facebook returns corresponding Facebook pixel code for the advertiser to incorporate into its website.

57. Facebook introduced its Pixel tracking tool in 2013 to allow online businesses like Defendant to track the actions of their users, subscribers, and customers on their websites, and importantly, to build detailed, valuable profiles about their website users.[10] *See* Meta, *Meta Pixel*, *available at* https://developers.facebook.com/docs/meta-pixel/ (last visited Dec. 12, 2024).

58. Meta describes the Meta Pixel as "a snippet of JavaScript code that allows you to track visitor activity on your website. It works by loading a small library of functions which you can use whenever a site visitor takes an action (called an event) that you want to track (called a conversion). Tracked conversions appear in the Ads Manager where they can be used to measure the effectiveness of your ads, to define custom audiences for ad targeting, for Advantage+ catalog ads campaigns, and to analyze that effectiveness of your website's conversion funnels." *See* Meta, Meta Pixel, *available at* https://developers.facebook.com/docs/meta-pixel/ (last visited Dec. 12, 2024).

[10] Meta, Meta Pixel, *available at* https://developers.facebook.com/docs/meta-pixel/ (last visited June 3, 2025).

59. Once activated, the Meta Pixel "tracks the people and type of actions they take,"[11] including each page users' visit, what buttons they click, as well as specific information that users input into a website.[12]

60. Meta explains that installing the Pixel allows them to "track Facebook ad-driven visitor activity on [their] website" and enables Facebook "to match . . . website visitors to their respective Facebook User accounts."[13]

61. In its "Get Started" page, Meta explains "[b]y default, the Pixel will track URLs visited, domains visited, and the devices your visitors use."[14] In addition, website operators can also program their Pixel to track "conversions" (website visitor actions) which are sent to the Facebook Ads Manager and the Facebook Events Manager to be used to analyze the effectiveness of ad campaigns and to define custom audiences to adjust and create new campaigns.[15]

62. Meta's "Get Started" page further explains how it can identify website visitors and match them to their Facebook pages: "[The Meta Pixel] relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can tally their actions in the Facebook Ads Manager so you can use the data to analyze your website's conversion flows and optimize your ad campaigns."

---

[11] Meta, Overview, *available at* https://www.facebook.com/business/goals/retargeting (last visited June 3, 2025).
[12] Meta, About Meta Pixel, *available at* https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited June 3, 2025).
[13] Meta, Get Started, *available at* https://developers.facebook.com/docs/meta-pixel/get-started (last visited June 3, 2025).
[14] Meta for Developers, Get Started, Meta (2024), *available at* https://developers.facebook.com/docs/meta-pixel/get-started (last visited Dec 12, 2024)
[15] Meta for Developers, Conversion Tracking, Meta (2024) *available at* https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking/ (last visited Dec 12, 2024)

63. Facebook maintains vast amounts of data on each of its users', like Plaintiff and the putative members of the Class.

64. This data is not limited to only what a person does on Facebook but also includes all records relating to when a user is tracked on off-Facebook websites – such as Plaintiff's interactions with www.reuters.com.

65. Facebook Pixels continuously add data from new interactions to the historical profiles Meta maintains on individuals with Facebook profiles.

66. Each interaction sent to Meta via the Pixel (including interactions sent by www.reuters.com), is linked to all of the other personal information Meta possesses about the user, such that Defendant has access to and can leverage a user's personal data.

67. In addition to the information every user is required to provide to Meta when creating an account (including First and Last name, date of birth, gender, email address and/or mobile number, and password), Meta also possesses and has access to all of the information every user has ever posted on his or her Facebook profile, profile views, likes, comments, shares and/or re-posts, event invitations, event R.S.V.P.'s, Facebook messages, "check-ins," and much, much more. Further, as explained above, Facebook maintains a record of each user's Off-Facebook Activity – all Facebook Pixel events that "fire" on non-Facebook websites, including www.reuters.com.

68. Crucial to the Pixel's effectiveness is its ability to associate a user's interactions on websites across the internet with that specific user's unique Facebook profile. The Pixel's fundamental purpose is to continuously add data from new interactions to the historical profiles Meta maintains on individuals with Facebook profiles (and even for a time after users delete their Facebook profiles).

69. Each interaction sent to Meta via the Pixel (including by the Defendant from www.reuters.com), is linked to all of the other personal information Meta possesses about the user, and this constant addition of data aids Meta – one of the worst data-privacy actors of this generation...if not ever – in targeting users.

70. Thus, for each of Plaintiff's interactions on the Website, the Pixel transmitted those interactions to Meta, who was able to instantaneously associate that interaction with Plaintiff's personal information that he submitted when creating her account, and any personal information ever available on his Facebook profile.

71. Facebook also creates "shadow profiles," of users and at least one court has recognized that a pixel's ability to track comprehensive browsing history is important. *See, e.g., Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1078-79 (N.D. Cal. 2021) (finding a reasonable expectation of privacy where Google combined the unique identifier of the user it collects from websites and Google Cookies that it collects across the internet on the same user).[16]

72. Once a company or organization has installed the Meta Pixel on its website, the Pixel tracks users as they navigate through the website and logs a variety of information designated for tracking by the company, including pages visited, any website "buttons" they click, the specific information entered in forms (including personal information), as well as "optional values."[17]

[16] *See* Facebook Shadow Profiles (Feb. 2022), *available at* https://www.cesifo.org/DocDL/cesifo1_wp9571.pdf (last visited June 3, 2025)

[17] Meta, Meta Pixel, *available at* https://developers.facebook.com/docs/meta-pixel/ (last visited June 3, 2025).

73. Websites and apps use Facebook's pixel and SDK to collect information about user's devices and activities and send that to Facebook. Facebook then uses that information to show the user targeted ads.

74. To obtain the code for the Pixel, the website advertiser tells Facebook which website events it wants to track (*e.g.*, Video Media) and Facebook returns corresponding Facebook pixel code for the advertiser to incorporate into its website.

75. Defendant installed the Facebook tracking pixel, which enables it to disclose Plaintiff's and Class Members' Personal Viewing Information to Facebook, because it benefits financially from the advertising and information services that stem from use of the Pixel.

76. When a digital subscriber enters the website www.reuters.com, navigates to, and then watches Video Media on the website, the website sends to Facebook information about the viewer, including, but not limited to, their identity and the media content the digital subscriber watched.

77. Specifically, www.reuters.com sends to Facebook the video content name, the URL of the pre-recorded video that was viewed (which clearly identified the video content being watched) along with, most notably, the viewers' Facebook ID that uniquely identifies the user Defendant's website does this because Defendant made the knowing choice to configure the tracking technologies on its site to function in this manner.

78. To "implement the pixel" on its website, Defendant had to take several affirmative steps. For example, Facebook notes: "To install the Pixel, we highly recommend that you add its base code between the opening and closing <head> tags on every page where you will be tracking website visitor actions. Most developers add it to their website's persistent header, so it can be used on all pages." *See* Meta for Developers, *Get Started*, *Installing the*

Pixel, *available at* https://developers.facebook.com/docs/meta-pixel/get-started (last visited May 1, 2025) (formatting in original).

79. Moreover, Facebook notes that "[d]evelopers and marketers can ***optionally choose*** to send additional information about the visit through Custom Data events." *See* Facebook, *Meta Pixel*, *available at* https://developers.facebook.com/docs/meta-pixel (last visited May 1, 2025). Thus, Defendant made a conscious decision to share its users' PII to Meta. This awareness is demonstrated by several factors, including: (a) the fundamental purpose and functionality of the Pixel, which is designed to collect data on user interactions with a website, (b) the widespread public information and media coverage regarding Meta's advertising practices, making these practices widely known, and (c) the resources and documentation provided by Meta on its website, where users like the Defendant can access information about the Pixel's capabilities and obtain the necessary code to implement it on their own websites.

80. At all relevant times, the Defendant was aware that the Pixel transmits PII to Meta. This awareness is demonstrated by several factors, including: (a) the fundamental purpose and functionality of the Pixel, which is designed to collect data on user interactions with a website, (b) the widespread public information and media coverage regarding Meta's advertising practices, making these practices widely known, and (c) the resources and documentation provided by Meta on its website, where users like the Defendant can access information about the Pixel's capabilities and obtain the necessary code to implement it on their own websites.

81. The Defendant's awareness of the Pixel is further demonstrated by the benefits it derived from the Pixel's functionality.

82. By installing the Pixel, the Defendant was able to target digital advertising to its subscribers, as well as potential subscribers, based on the content those individuals had

previously accessed or requested from the website, including prerecorded audiovisual materials.[18]

83. Defendant specifically benefited from its installation of the Pixels because Defendant maintains a Facebook page (www.facebook.com/reuters) and advertises on Facebook, meaning its disclosure of users' interactions to Meta ensured its ads were shown to the right individuals on Facebook at exactly the right time.

84. Defendant is the sole operator of the Website, and Defendant is solely responsible for the decisions it makes about what technology to include within its Website. Defendant made the affirmative decision to knowingly include the Meta Pixel on its website.

85. Defendant knew and understood what the Pixel was, how it functioned, and what data it would collect and share with Meta because Defendant installed the Pixel on its site and configured its functionality.

~~33.~~

~~34.~~86. Defendant installed the Facebook tracking pixel, which enables it to disclose Plaintiff's and Class Members' Personal Viewing Information to Facebook, because it benefits financially from the advertising and information services that stem from use of the pixel. When a ~~R~~www.reuters.com digital subscriber enters the website and watches Video Media on the website, the website sends to Facebook certain information about the viewer, including, but not limited to, their identity and the media content the digital subscriber watched. Specifically, ~~R~~www.reuters.com sends to Facebook the video content name, its URL, and, most notably, the viewers' Facebook ID.

[18] Meta for Developers, Conversion Tracking, Meta for Developers (2024), *available at* https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking/ (last visited June 3, 2025).

2. Facebook ID ("FID")

87. An FID is a unique and persistent identifier that Facebook assigns to each user. With it, anyone ordinary person can look up the user's Facebook profile and name. When a Facebook user with one or more personally identifiable FID cookies on their browser views Video Media from ~~R~~ www.reuters.com on the website or app, ~~R~~ www.reuters.com, through its website code, causes the digital subscribers identity and viewed Video Media to be transmitted to Facebook by the user's browser. This transmission is not the digital subscribers' decision, but results from Defendant's purposeful use of its Facebook tracking pixel by incorporation of that pixel and code into ~~R~~ www.reuters.com's website or App. Defendant could easily program the website and app so that this information is not automatically transmitted to Facebook when a subscriber views Video Media. However, it is not Defendant's financial interest to do so because it benefits financially by providing this highly sought-after information.

88. Every Facebook account is assigned a unique User ID—commonly known as the "Facebook ID" or "FID" field—which links directly to a specific user's profile regardless of the name, alias, or other personal information publicly displayed on the account. This information, and other information, is transmitted to Facebook being a data file called the "c_user_" cookie. This User ID functions as a persistent identifier that uniquely distinguishes one account from all others on the Facebook platform. ~~Every Facebook account is assigned a unique User ID—commonly known as the "c_user" field—which links directly to a specific user's profile regardless of the name, alias, or other personal information publicly displayed on the account. This User ID functions as a persistent identifier that uniquely distinguishes one account from all others on the Facebook platform.~~

89. Facebook itself publishes explanations and help-center materials confirming that a User ID is a string of numbers that connects to a specific profile and can be entered into the URL bar (e.g., "www.facebook.com/[UserID]") to navigate directly to that profile. Ordinary Internet users — roughly seven in ten -Americans – are among Facebook's user base and regularly encounter URLs and learn from Facebook's own "Help" pages how to find and use User IDs.[19]

90. A simple online search for "how to find Facebook account with Facebook ID" immediately yields publicly available instructions, demonstrating that even non-technical users can, without specialized knowledge, discover and apply a User ID to locate a given Facebook profile.

91. In modern internet use, average individuals see and click URLs dozens or hundreds of times per day across email, news articles, social media, and other web pages.

92. Upon seeing a string beginning "http" or "www," an ordinary person understands that it can be entered into a browser to access the linked resource.

93. When a URL embedding a Facebook User ID is disclosed — such as by a video service provider — any ordinary user who follows that link will be brought directly to the Facebook profile operating under that ID, thereby identifying the person who watched the video and revealing any public details displayed on that profile (e.g., photos, posts, "friends", location, occupation, partner/spouse, educational history, etc.).

94. A Facebook User ID identifies an individual with far greater precision than a name alone, particularly where the name is common or duplicated. For example, while multiple individuals named "John Smith" may exist in the United States—or even on Facebook—only

[19] https://www.pewresearch.org/short-reads/2024/02/02/5-facts-about-how-americans-use-facebook-two-decades-after-its-launch/ (last visited May 8, 2025)

one account will correspond to a particular User ID. Thus, possession of the User ID allows identification of a unique individual with certainty.

95. Even if a profile's displayed name is pseudonymous (e.g., "Anony Mous"), the underlying User ID still furnishes a clear hook by which third parties can associate specific viewing behavior with a single, uniquely identified human being.

96. Thus, a Facebook User ID is not an obscure technical detail but a readily accessible identifier that ordinary people understand and use to connect personal names, profiles, and online activities.

97. The FID disclosure enables direct linkage of an individual to particular content they have viewed, rendering any assertion of anonymity baseless.

98. Facebook maintains internal user interfaces that automatically translate incoming Pixel transmissions—including the c_user value and video metadata—into readable, plain-text formats. These interfaces allow Facebook to view and analyze incoming data in human-understandable terms, such as identifying which user watched which video. Although these internal tools are not publicly available, their existence is evidenced by Facebook's technical documentation and operational capabilities, which rely on the ingestion and automated interpretation of Pixel data to serve ads and build user profiles.

99. Indeed, even the website operators who implement the Facebook Pixel have access to dashboards and analytics tools that display Pixel outputs in clear, non-technical terms (e.g., "User watched [Video Title]"). These tools confirm that both Facebook and its business partners interpret the underlying code using accessible interfaces designed to reveal user behavior in plain English.

100. While the technical evidence in this case may show the code-based transmission of a Facebook User ID and video title, Facebook would not need to read or interpret that code manually. Instead, it receives and processes the information through internal systems that automatically extract the meaning of the data—linking a specific user to a specific video—with ease and accuracy.

101. Furthermore, with the rise in General Artificial Intelligence agents such as ChatGPT, anyone with an internet connection can use tools to decipher strings of computer code.

102. In other words, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to any Facebook profile. Simply put, with only an FID and the video content name and URL – all of which Defendant knowingly and readily provides to Facebook without any consent from the digital subscribers – any ordinary person could learn the identity of the digital subscriber and the specific video or media content they requested on www.reuters.com.

103. Additionally, Facebook stores pixel event and other data in Hive tables – internal data storage that is used for large-scale data processing and analytics.

104. Facebook then joins the information across different Hive tables.

105. Facebook can and does identify, process, and use pixel data, via one or more Hive tables (of which there are tens of millions), to understand the domain from which data was originated and what "event" triggered the data disclosure.

106. Said differently, Facebook understands who is sending it data via the Facebook pixel, and, further, understands what the event data means

At all relevant times, Defendant knew that the Facebook pixel disclosed Personal Viewing Information to Facebook. This was evidenced from, among other things, the functionality of the pixel, including that it enabled www.reuters.com and an accompanying app to show targeted advertising to its digital subscribers based on the products those digital subscribers had previously viewed on the website or app, including Video Media consumption, for which Defendant received financial remuneration.

~~35.~~107.

~~36. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to any Facebook profile. Simply put, with only an FID and the video content name and URL—all of which Defendant knowingly and readily provides to Facebook without any consent from the digital subscribers—any ordinary person could learn the identity of the digital subscriber and the specific video or media content they requested on Reuters.com.~~

~~37. At all relevant times, Defendant knew that the Facebook pixel disclosed Personal Viewing Information to Facebook. This was evidenced from, among other things, the functionality of the pixel, including that it enabled Reuters.com and accompanying app to show targeted advertising to its digital subscribers based on the products those digital subscriber's had previously viewed on the website or app, including Video Media consumption, for which Defendant received financial remuneration.~~

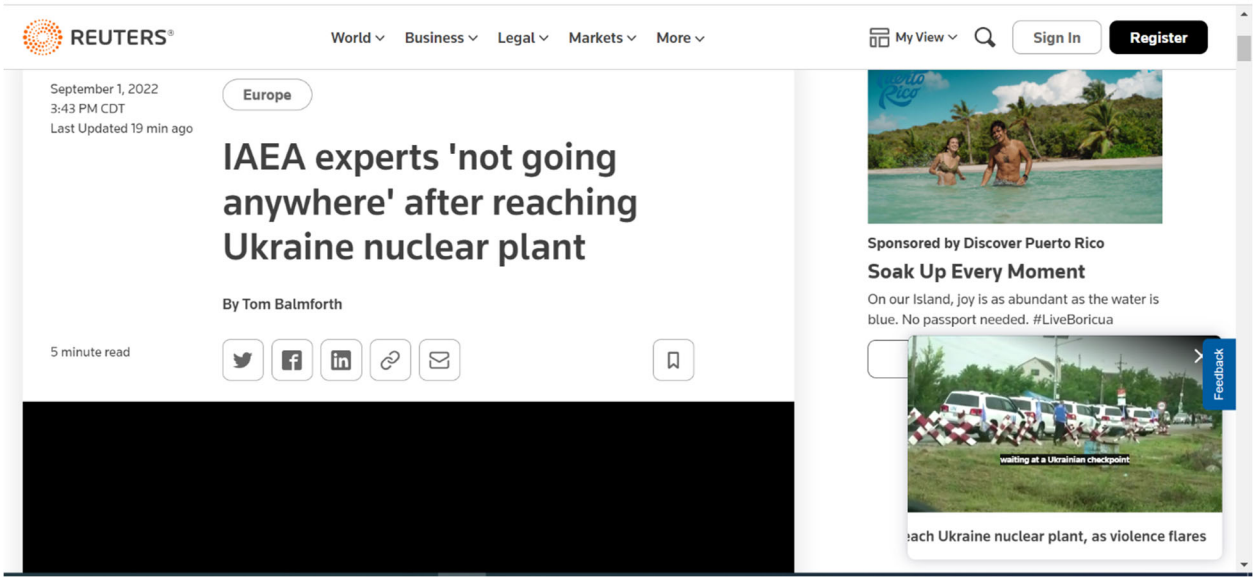
E. Reuters.com Unlawfully Discloses Its Digital Subscribers' Personal Viewing Information to Facebook

~~38.~~108. Defendant maintains a vast digital database comprised of its digital subscribers' Personal Viewing Information, including the names and e-mail addresses of each digital subscriber and information reflecting the Video Media that each of its digital subscribers viewed.

~~39.~~109. Defendant is not sharing anonymized, non-personally identifiable data with Facebook. To the contrary, the data it discloses is tied to unique identifiers that track specific Facebook users. Importantly, the recipient of the Personal Viewing Information – Facebook – receives the Personal Viewing Information as one data point. Defendant has thus monetized its database by disclosing its digital subscribers' Personal Viewing Information to Facebook in a manner allowing it to make a direct connection – without the consent of its digital subscribers and to the detriment of their legally protected privacy rights.

~~40.~~110. Critically, the Personal Viewing Information Defendant discloses to Facebook allows Facebook to build from scratch or cross-reference and add to the data it already has in their own detailed profiles for its own users, adding to its trove of personally identifiable data.

~~41.~~111. These factual allegations are corroborated by publicly available evidence. For instance, as shown in the screenshot below, a user visits ~~R~~ www.reuters.com and clicks on an article titled "IAEA experts 'not going anywhere' after reaching Ukraine nuclear plant" and watches the video in the article.



Pictured above: The article titled "IAEA experts 'not going anywhere' after reaching Ukraine nuclear plant" (taken from ~~R~~ www.reuters.com on or about September 8, 2022).

~~42.~~112. As demonstrated below, once the user clicks on and watches the video in the article, ~~R~~ www.reuters.com sends the content name of the video the digital subscriber watched, the URL, and the digital subscriber's FID to Facebook.

HTTP single communication session sent from the device to Facebook, reveals the video name, URL and the viewer's FID (c_user field)

~~43.~~113. As a result of Defendant's data compiling and sharing practices, Defendant has knowingly disclosed to Facebook for its own personal profit the Personal Viewing Information of Defendant's digital subscribers, together with additional sensitive personal information.

114. Defendant disclosed PII within the meaning of VPPA because the information transmitted to Facebook—including users' FIDs and specific video file names—was disclosed in a technical format, but one that is understood by ordinary people.

115. The disclosing party here used Facebook's PageView code to transmit FIDs and video content identifiers directly to Facebook but did so in a manner that is easily decipherable (again, presuming an ordinary person can read). Much like a person does not need to understand precisely how radio waves work to hear the radio play, or understand the words coming out of the radio

~~44.~~116. Defendant does not seek its digital subscribers' prior written consent to the disclosure of their Personal Viewing Information (in writing or otherwise) and its customers remain unaware that their Personal Viewing Information and other sensitive data is being disclosed to Facebook.

~~45.~~117. By disclosing its digital subscribers Personal Viewing Information to Facebook – which undeniably reveals their identity and the specific video materials they requested from Defendant's website – Defendant has intentionally and knowingly violated the VPPA.

F. Disclosing Personal Viewing Information is Not Necessary

~~46.~~118. Tracking pixels are not necessary for Defendant to operate ~~R~~ www.reuters.com's digital news publications and sign-up digital subscriptions. They are deployed on Defendant's website for the sole purpose of enriching Defendant and Facebook.

~~47.~~119. Even if an on-line news publication found it useful to integrate Facebook tracking pixels, Defendant is not required to disclose Personal Viewing Information to Facebook. In any event, if Defendant wanted to do so, it must first comply with the strict requirements of VPPA, which it failed to do.

G. Plaintiff's Experiences

~~48.~~120. Plaintiff Christina Leslie has been a digital subscriber of ~~R~~ www.reuters.com from 2022 to the present. Plaintiff became a digital subscriber of ~~R~~ www.reuters.com by providing, among other information, her email address and IP address (which informs Defendant as to the city and zip code she resides in as well as her physical location), and any cookies associated with her device. As part of her subscription, she receives emails and other communications from ~~R~~ www.reuters.com.

121. Plaintiff has had a Facebook account since approximately 2012. From 2022 to the present, Plaintiff viewed Video Media via ~~R~~ www.reuters.com website and App.

122. When she created her Facebook profile, Plaintiff provided Meta with the required information to create her profile: his name, date of birth, gender, contact information, and password.

123. During the relevant period, Plaintiff's Facebook profile included information specifically and uniquely identifying her, including but not limited to her full name, personal photographs that contain location and other information, and likes and follows of certain commercial establishments in her hometown. Plaintiff's Facebook profile was accessible to any

person in possession of her unique FID (which Facebook maintains for every user). Any person (or corporation) could use her FID to load Plaintiff's Facebook page directly and see this available information that specifically and uniquely identifies her.

124. Additionally, Facebook, sitting in possession of Plaintiff's entire Facebook profile and account history, was in a special position. It could not only directly identify Plaintiff, but it could also access her entire historical Facebook dataset, including her visits to www.reuters.com and information disclosing that she had viewed specific video content.

125. Plaintiff was a subscriber to www.reuters.com and is therefore a "consumer" under the VPPA.

126. Plaintiff requested, obtained, and/or watched prerecorded audio visual material on ww.reuters.com and through her digital subscription to Defendant's services.

~~49.~~127. During the period when Plaintiff was a subscriber to the Defendant's services, she maintained a Facebook profile. Defendant knowingly shared her Facebook ID (FID) with Meta, along with the titles of the prerecorded audiovisual materials she accessed or requested (frankly, Defendant went one step further and denoted a "watch" in its URLs, which it shared with Facebook) and the URLs for those videos.

~~50.~~128. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Personal Viewing Information to Facebook. Plaintiff has never been provided any written notice that Defendant discloses its digital subscribers' Personal Viewing Information, or any means of opting out of such disclosures of her Personal Viewing Information. Defendant nonetheless knowingly disclosed Plaintiff's Personal Viewing Information to Facebook.

~~51.~~129. Because Plaintiff is entitled by law to privacy in her Personal Viewing Information, Defendant's disclosure of her Personal Viewing Information deprived Plaintiff of the full set of benefits to which she is entitled. Plaintiff did not discover that Defendant disclosed her Personal Viewing Information to Facebook until August 2022.

CLASS ACTION ALLEGATIONS

~~52.~~130. Plaintiff brings this action individually and on behalf of all others similarly situated as a class action under Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of the following class (the "Class"):

> All persons in the United States with a digital subscription to an online website owned and/or operated by Defendant that had their Personal Viewing Information disclosed to Facebook by Defendant.

~~53.~~131. Excluded from the Class are Defendant, their past or current officers, directors, affiliates, legal representatives, predecessors, successors, assigns and any entity in which any of them have a controlling interest, as well as all judicial officers assigned to this case as defined in 28 USC § 455(b) and their immediate families.

~~54.~~132. Numerosity. Members of the Class are so numerous and geographically dispersed that joinder of all members of the Class is impracticable. Plaintiff believes that there are hundreds of thousands of members of the Class widely dispersed throughout the United States. Class members can be identified from Defendant's records and non-party Facebook's records.

~~55.~~133. Typicality. Plaintiff's claims are typical of the claims of members of the Class. Plaintiff and members of the Class were harmed by the same wrongful conduct by Defendant in that Defendant caused Personal Viewing Information to be disclosed to Facebook without obtaining express written consent. her claims are based on the same legal theories as the claims of other Class members.

~~56.~~134. Adequacy. Plaintiff will fairly and adequately protect and represent the interests of the members of the Class. Plaintiff's interests are coincident with, and not antagonistic to, those of the members of the Class. Plaintiff is represented by counsel with experience in the prosecution of class action litigation generally and in the emerging field of digital privacy litigation specifically.

~~57.~~135. Commonality. Questions of law and fact common to the members of the Class predominate over questions that may affect only individual members of the Class because Defendant has acted on grounds generally applicable to the Class. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Classes include:

a. Whether Defendant knowingly disclosed Class members' Personal Viewing Information to Facebook;

b. Whether the information disclosed to Facebook concerning Class members' Personal Viewing Information constitutes personally identifiable information under the VPPA;

c. Whether Defendant's disclosure of Class members' Personal Viewing Information to Facebook was knowing under the VPPA;

d. Whether Class members consented to Defendant's disclosure of their Personal Viewing Information to Facebook in the manner required by 18 U.S.C. § 2710(b)(2)(B); and

e. Whether the Class is entitled to damages as a result of Defendant's conduct.

~~58.~~136. Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not

practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiff knows of no special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

CLAIM FOR RELIEF

FIRST CLAIM FOR RELIEF

Violation of the Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710

~~59.~~137. Plaintiff incorporates the preceding paragraphs by reference as if fully set forth herein.

~~60.~~138. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally-identifying information" concerning any consumer to a third-party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C § 2710.

~~61.~~139. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials."

~~62.~~140. Defendant is a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because it engaged in the business of delivering audiovisual materials that are similar to prerecorded video cassette tapes and those sales affect interstate or foreign commerce.

~~63.~~141. As defined in 18 U.S.C. § 2710(a)(3), "personally-identifiable information" is defined to include "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."

~~64.~~142. Defendant knowingly caused Personal Viewing Information, including FIDs, concerning Plaintiff and Class members to be disclosed to Facebook. This information constitutes personally identifiable information under 18 U.S.C. § 2710(a)(3) because it identified

each Plaintiff and Class member to Facebook as an individual who viewed ~~R~~www.reuters.com Video Media, including the specific video materials requested from the website.

~~65.~~143. As defined in 18 U.S.C. § 2710(a)(1), a "consumer" means "any renter, purchaser, or subscriber of goods or services from a video tape service provider." As alleged in the preceding paragraphs, Plaintiff subscribed to a digital ~~R~~ www.reuters.com plan that provides Video Media content to the digital subscriber's desktop, tablet, and mobile device. Plaintiff is thus a "consumer" under this definition.

~~66.~~144. As set forth in 18 U.S.C. § 2710~~9~~(b)(2)(B), "informed, written consent" must be (1) in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer; and (2) at the election of the consumer, is either given at the time the disclosure is sought or given in advance for a set period of time not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner." Defendant failed to obtain informed, written consent under this definition.

~~67.~~145. In addition, the VPPA creates an opt-out right for consumers in 18 U.S.C. § 2710(2)(B)(iii). It requires video tape service providers to also "provide[] an opportunity for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election." Defendant failed to provide an opportunity to opt out as required by the VPPA.

~~68.~~146. Defendant knew that these disclosures identified Plaintiff and Class members to Facebook. Defendant also knew that Plaintiff's and Class members' Personal Viewing Information was disclosed to Facebook because, inter alia, Defendant chose, programmed, and intended for Facebook to receive the video content name, its URL, and, most notably, the digital subscribers' FID.

~~69.~~147. By disclosing Plaintiff's and the Class's Personal Viewing Information, Defendant violated Plaintiff's and the Class members' statutorily protected right to privacy in their video-watching habits. *See* 18 U.S.C. § 2710(c).

~~70.~~148. As a result of the above violations, Defendant is liable to the Plaintiff and other Class members for actual damages related to their loss of privacy in an amount to be determined at trial or alternatively for "liquidated damages not less than $2,500 per plaintiff." Under the statute, Defendant is also liable for reasonable attorney's fees, and other litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

VII. RELIEF REQUESTED

~~71.~~149. Accordingly, Plaintiff, individually and on behalf of the proposed Class, respectfully requests that this court:

a. Determine that this action may be maintained as a class action pursuant to Fed R. Civ. P. 23(a), (b)(2), and (b)(3) and declare Plaintiff as the representative of the Class and Plaintiff's Counsel as Class Counsel;

b. For an order declaring that Defendant's conduct as described herein violates the federal VPPA, 18 U.S.C. § 2710(c)(2)(D);

c. For Defendant to pay $2,500.00 to Plaintiff and each Class member, as provided by the VPPA, 18 U.S.C. § 2710(c)(2)(A);

d. For punitive damages, as warranted, in an amount to be determined at trial, 18 U.S.C. § 2710(c)(2)(B);

e. For prejudgment interest on all amounts awarded;

f. For an order of restitution and all other forms of equitable monetary relief;

g. For injunctive relief as pleaded or as the Court may deem proper; and

h. For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit, 18 U.S.C. § 2710(c)(2)(C).

JURY DEMAND

~~72.~~150. Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff, individually and on behalf of the proposed Class, demands a trial by jury on all issues so triable.

~~Dated:~~ ~~September 15, 2022~~May 15, 2025

Respectfully Submitted:

By: */s/ Michael L. Murphy*
Michael L. Murphy (NY 5084397)
BAILEY & GLASSER LLP
1055 Thomas Jefferson Street NW
Suite 540
Washington, DC 20007
T: 202.494.3531
mmurphy@baileyglasser.com

Brandon M. Wise – IL Bar # 6319580*
PEIFFER WOLF CARR
KANE CONWAY & WISE, LLP
One US Bank Plaza, Suite 1950
St. Louis, MO 63101
T: 314.833.4827
bwise@peifferwolf.com

**pro hac vice*

Counsel for Plaintiff and the Putative Class